A (linear) algebraic group is, roughly, a group of matrices (under matrix multiplication) that consists of all matrices whose entries obey some polynomial equations.

We'll work with matrices having entries in any field $K$.

**Def:** Let $M(n,K)$ be the vector space of $n \times n$ matrices with entries in $K$. We'll write $M(n)$ for short.

**Def:** Let the general linear group $GL(n,K)$ be the group of all invertible $n \times n$ matrices with entries in $K$:

$$GL(n,K) = \{ g \in M(n,K) : \det(g) \neq 0 \}$$

We'll write $GL(n)$ for short.

**Def:** A (linear) algebraic group is a subgroup of $GL(n,K)$ of this form:

$$G = \{ g \in GL(n,K) : P_1(g) = \cdots = P_N(g) = 0 \}$$

where $P_i : M(n,K) \to K$ are polynomials in the matrix entries.

(This is just a first version of the definition; see Springer for other equivalent definitions. Allowing infinitely many polynomial equations would not change anything, since polynomial rings are Noetherian).

Examples of algebraic groups:

1. $GL(n,K)$ is the king of all algebraic groups!

2. Let $SL(n,K)$ (or $SL(n)$) be the special linear group:

$$SL(n,K) = \{ g \in GL(n,K) : \det(g) = 1 \}$$

This is an algebraic group because det is a polynomial. This partially eliminates the center of $GL(n,K)$: the center of $SL(n,K)$ is just the matrices

$$\begin{pmatrix} \alpha & & 0 \\ & \alpha & \\ & \ddots & \\ 0 & & \alpha \end{pmatrix} \qquad \text{s.t. } \alpha^n = 1,$$

so it's finite. We'll find out why we want to get rid of the center later.

3. Let $O(n,K)$ (or $O(n)$ for short) be the orthogonal group:

$$O(n,K) = \{ g \in GL(n,K) : gv \cdot gw = v \cdot w, \ \forall\, v,w \in K^n \}$$

where $v \cdot w = \sum_{i=1}^{n} v_i \cdot w_i$.

Note: We could also write $O(n,K) = \{ g \in GL(n,K) : g^T g = 1 \}$ where $g^T$ is the transpose of $g$. This makes it more clear that $O(n,K)$ is actually an algebraic group, since it's defined by $n^2$ quadratic equations.

$$\left( gv \cdot gw = v \cdot w \iff v \cdot g^T g w = v \cdot w \iff g^T g = 1 \right)$$

Intuitively, $O(n)$ consists of rotations, reflections, and products of those. A typical reflection is:

$$\begin{pmatrix} -1 & & & \\ & 1 & & 0 \\ & & \ddots & \\ & 0 & & 1 \end{pmatrix}$$

4. If $g \in O(n)$, $\det(g^T g) = 1$, so $\det(g) = \pm 1$. So there's an algebraic group called the <u>special orthogonal</u> group:

$$SO(n,K) := O(n,K) \cap SL(n,K)$$

$$= \{ g \in GL(n,K) : g^T g = 1 \text{ and } \det(g) = 1 \}.$$

Note that in general, the intersection of linear algebraic groups in $GL(n,K)$ is again algebraic, as seen here.

$SO(n)$ consists only of rotations.

5. The <u>Euclidean group</u> $E(n,K)$ (or $E(n)$ for short) is the group of all maps $f: K^n \to K^n$ of the form

$$f(x) = Rx + v$$

where $R \in SO(n,K)$ is a rotation and $v \in K^n$ gives a translation.

For $n=2$, $K=\mathbb{R}$, this is the symmetry group of the Euclidean plane. It's a group because:

$$R(R'x+v')+v = (RR')x + (Rv'+v);\ R,R' \in SO(n),\ v,v' \in K^n.$$

So as a set $E(n) \cong SO(n) \times K^n$, is not isomorphic as groups though. Multiplication is instead given by

$$(R,v)(R',v') = (RR', Rv'+v)$$

It's not then a product of groups; instead it's a "semidirect product." To make $E(n)$ into an algebraic group, we need to think of $(R,v)$ as a matrix:

$$\phi : (R,v) \longmapsto \left(\begin{array}{c|c} R & v \\ \hline 0 \cdots 0 & 1 \end{array}\right)\Bigg\}_{n+1}$$

$$\underbrace{\qquad\qquad}_{n+1}$$

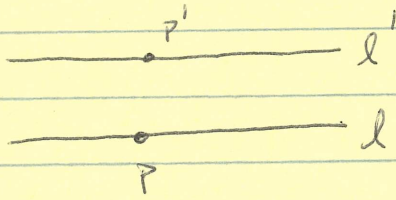
and check $\phi((R,v)(R',v')) = \phi(R,v)\cdot\phi(R',v')$. So now the group operation is matrix multiplication, and we get a subgroup of $GL(n+1,K)$ that's isomorphic to $E(n)$. So now we'll say

$$E(n) = \left\{ g \in GL(n+1) : g = \begin{pmatrix} R & v \\ 0 \cdots 0 & 1 \end{pmatrix},\ R \in SO(n),\ v \in K^n \right\}$$

and this is an algebraic group. Indeed, Euclidean geometry and its generalizations led to the modern theory of algebraic groups.

Euclidean geometry, with $E(2,\mathbb{R})$ as symmetries.

- Originally formulated as a bunch of axioms. One in particular caused trouble: the "parallel postulate", which says:



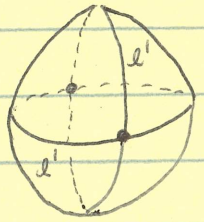

$$\forall p \in P, \forall \ell \in L \left( p \, I \, \ell \Rightarrow \forall p' \left( \neg p' I \ell \Rightarrow \exists! \ell' \in L \left( p' I \ell' \text{ and } \neg \exists q \left( q I \ell \text{ and } q I \ell' \right) \right) \right) \right)$$

where $I \subseteq P \times L$ is the relation called "incidence": $p I \ell$ means $p$ lies on $\ell$.

There are 2 kinds of geometry that obey all the axioms of Euclidean geometry except the parallel postulate:

i) elliptic geometry

$x^2+y^2+z^2=1$



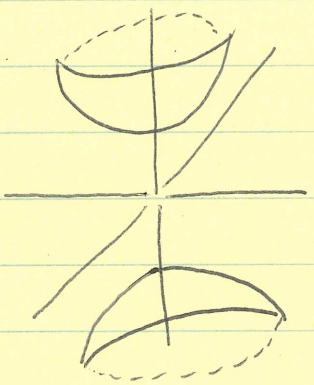

$P = \mathbb{R}P^2 = S^2/\sim$

$L = \{\text{great circles}\}$

Here there are no parallel lines: any two distinct lines intersect in a single point (after identifying antipodal points).

2) hyperbolic geometry

$x^2+y^2-z^2=1$

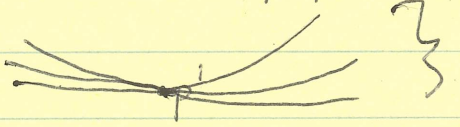


hyperboloid

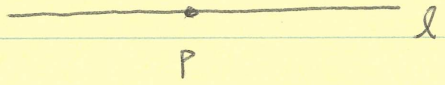
$$P = \{x^2+y^2-z^2=1\}/\{p\sim -p\}$$

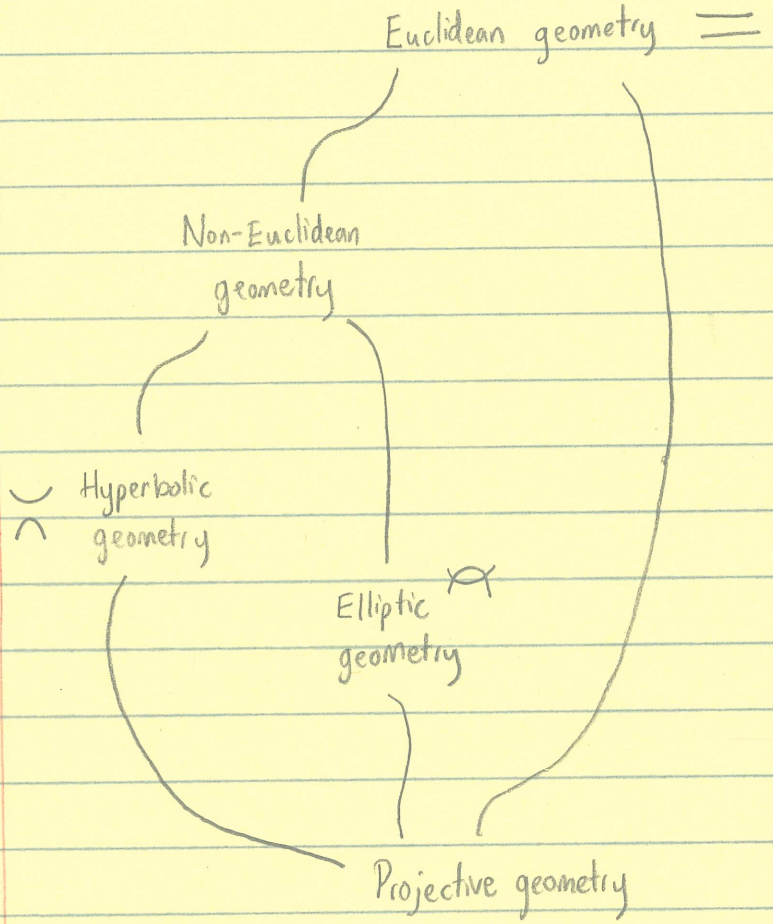
$L = \{$intersections of the hyperboloid with planes through origin$\}$

Here we have too many parallel lines:



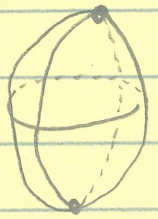
} many classes of $l'$






## 3 Geometries & Their Algebraic Groups

### 1) Elliptic Geometry



Take $K^3$ with the usual inner product:

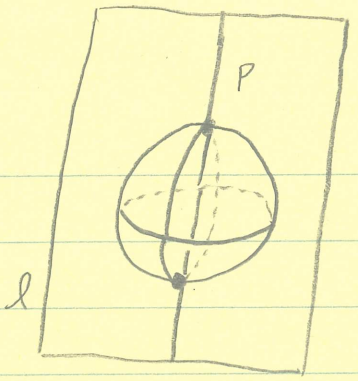
$$v \cdot w = v_1 w_1 + v_2 w_2 + v_3 w_3$$

Form the sphere:

$X = \{ v \in K^3 : v \cdot v = 1 \}$, and define a set $P$ of points and a set $L$ of lines as follows:

$P = \{ \text{1d-subspaces of } K^3 \}$

$L = \{ \text{2d-subspaces of } K^3 \}$

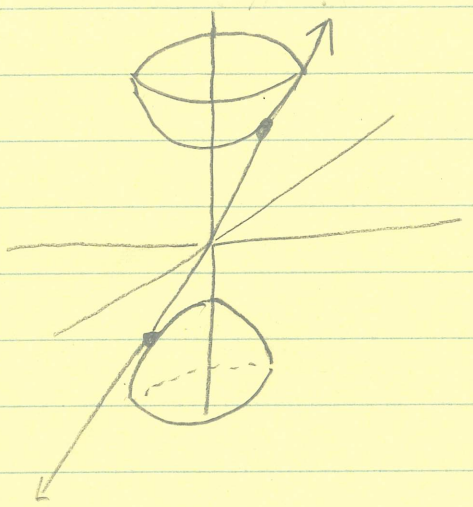



We define the incidence relation "a point $p$ lies on a line $\ell$" by $p \leq \ell$. We use the dot product to define distances and angles between points and lines resp.

The group $SO(3)$ acts on $K^3$ preserving the dot product, and thus it acts on $P$ and $L$ preserving distances and angles and also the incidence relation: $\forall g \in SO(3)$,

$$p \leq \ell \Rightarrow gp \leq g\ell$$

## 2) Hyperbolic geometry



Give $K^3$ the Lorentzian dot product:

$$v \cdot w = -v_1 w_1 - v_2 w_2 + v_3 w_3$$

so that

$X = \{ v \in K^3 : v \cdot v = 1 \}$ is a hyperboloid w/ two sheets.
Define sets of points and lines by

$P = \{$ 1d-subspaces of $K^3$ with non-empty intersection with $X\}$

$L = \{$ 2d-subspaces of $K^3$ with non-empty intersection with $X\}$

(Note the new clause compared with elliptic geometry - it's not really new, it was just "invisible" before)

Let

$O(1,2) = \{ g \in GL(3) : gv \cdot gw = v \cdot w, \forall v, w \in K^3 \}$ where $\cdot$ is the Lorentzian dot product.

Einstein realized that space and time form $\mathbb{R}^4$ with $O(1,3)$ acting as symmetries.

Let $SO(1,2) = O(1,2) \cap SL(3)$. Then $SO(1,2)$ acts on $K^3$ preserving the Lorentzian dot product, and thus it acts on $X$, $P$, and $L$. You can define distances between points and angles between lines and $SO(1,2)$ preserves these.

We say $p \in P$ lies on a line $\ell \in L$ if $p \subseteq \ell$, and then $SO(1,2)$ preserves this incidence relation: $\forall g \in SO(1,2)$,

$$p \subseteq \ell \Rightarrow gp \subseteq g\ell.$$

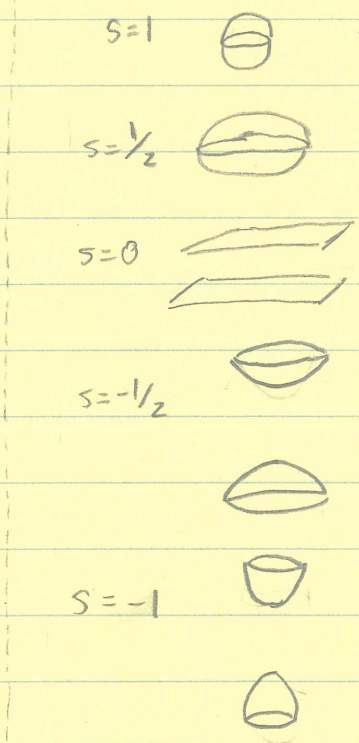
## 3) Euclidean Geometry

Take $k^3$ with the degenerate dot product:

$$v \cdot w = v_3 w_3$$

Note (looking at the bilinear forms in the different geometries here):

| | | | |
|---|---|---|---|
| elliptic | + | + | + |
| Euclidean | 0 | 0 | + |
| hyperbolic | − | − | + |




As s varies, get a different geometry

Now $X = \{v \in k^3 : v \cdot v = 1\}$ is the set $\{z^2 = 1\}$ : two parallel planes

So we let

$P = \{$1d-subspaces of $k^3$ having nonempty intersection with $X\}$

$L = \{$2d-subspaces of $k^3$ having nonempty intersection with $X\}$

The Euclidean group

$$E(3) = \left\{ \left(\begin{array}{c|c} R & v \\ \hline 0\,0 & 1 \end{array}\right) : R \in SO(2) \text{ and } v \in k^2 \right\}$$

acts on $k^3$ preserving $X = \{(x,y,z) \in k^3 : z = \pm 1\}$

$$\left(\begin{array}{c|c} R & v \\ \hline 0\,0 & 1 \end{array}\right) \cdot \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = \begin{pmatrix} R\begin{pmatrix} x \\ y \end{pmatrix} + v \\ 1 \end{pmatrix}$$

So $E(3)$ preserves the plane $z=1$ and acts on it just as a Euclidean transformation should:

$$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto R\begin{pmatrix} x \\ y \end{pmatrix} + v$$

$E(3)$ also preserves the plane $X = -1$, hence $X$. We can define distance b/w points and angles b/w lines, and $E(3)$ preserves these; it also preserves the incidence relation $p \subseteq \ell$. So the main weird thing about this case is that $E(3)$ is <u>not</u> the group of all $\det = 1$ transformations preserving the degenerate dot product. It's only the subgroup where $R \in SO(2) \subseteq SL(2)$.

People looked at the 3 geometries and noticed they're all subsumed (as far as incidence relations go) in a single geometry: projective geometry.

## 4) Projective Geometry

Here we define points and lines in a simpler way:

$$P = \{ \text{1d-subspaces of } k^3 \}$$

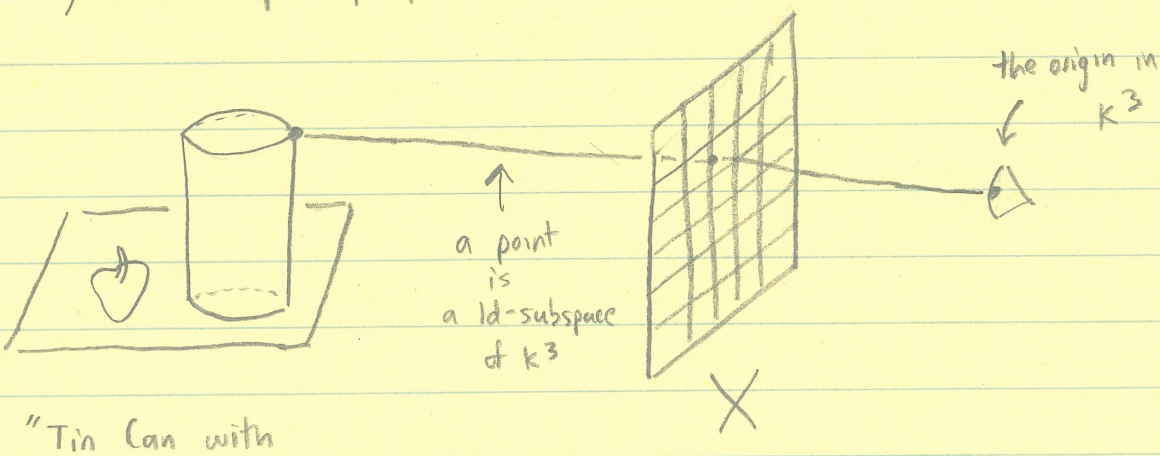
$$L = \{ \text{2d-subspaces of } k^3 \}$$

We won't define distances b/w points and angles b/w lines: all we care about is the incidence geometry: we say $p \in P$ is incident to $\ell \in L$ (or $p$ lies on $\ell$) if $p \subseteq \ell$.

Now the symmetry group is all of $GL(3)$: all invertible linear transf. - since all of them act on $P$ and $L$ preserving the incidence relation:

$$p \subseteq \ell \Rightarrow gp \subseteq g\ell$$

Actually, projective geometry goes back at least to the Renaissance painters, who developed perspective




"Tin Can with Apple"

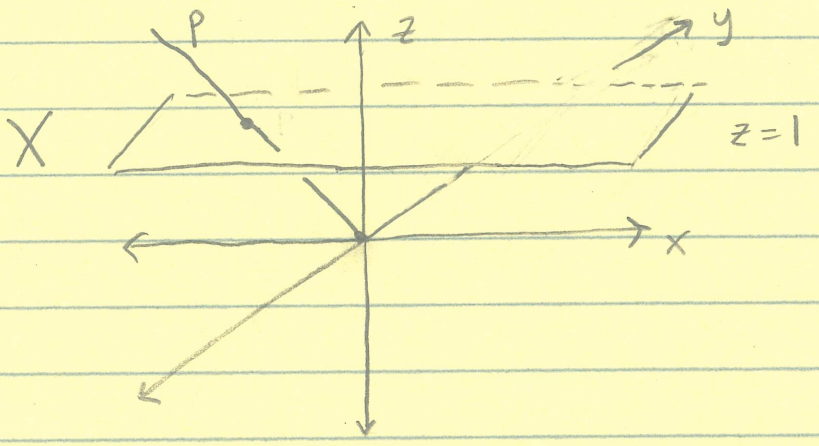
If we fix any plane $X \subseteq k^3$ not containing the origin, most (but not all) 1d-subspaces of $k^3$ will intersect $X$ in a single point (Some won't intersect of $X$ at all).

Thus most points $p \in P$ correspond to points of $X$. The remaining points of $P$ are called "points at infinity." Mathematically, we can do this trick in any dimension: start with $k^n$, and form a set of points called projective $(n-1)$ space:

$$kP^{n-1} = \{ \text{1d-subspaces of } k^n \}$$

Most points in $kP^{n-1}$ will intersect the plane

$$X = \{ (x_1, \dots, x_{n-1}, 1) : x_i \in k \}$$ in a single point.




So we get a 1-1 correspondence between $X$ and an "open dense" set in $kP^2$: only 1d-subspaces lying in xy-plane don't correspond to points of $X$.

Points and lines in either elliptic, hyperbolic or Euclidean geometry give points and lines in projective geometry, and their symmetry groups are all subgroups of its symmetry group $GL(3)$.

# Projective Geometry

Recall that for any field $k$,

$$KP^n = \{\text{1d-linear subspaces of } k^{n+1}\}$$

**Thm:** As sets, $KP^n \cong k^n + k^{n-1} + k^{n-2} + \cdots + k^0$. ($k^0 = \{0\}$)

Here, $\cong$ means there's a bijection and $+$ means disjoint union. These pieces $k^n, k^{n-1}, \ldots, k^0$ are called Schubert cells. This is called a Schubert decomposition.

**Pf:** Any 1d-subspace of $k^{n+1}$ has the form $\langle (x_1, \ldots, x_{n+1}) \rangle$ with $(x_1, \ldots, x_{n+1}) \neq 0$ - where $\langle\ \rangle$ means the span - all linear combinations.

If $x_{n+1} \neq 0$, $p = \langle \left(\frac{x_1}{x_{n+1}}, \frac{x_2}{x_{n+1}}, \ldots, \frac{x_n}{x_{n+1}}, 1\right) \rangle = \langle (y_1, \ldots, y_n, 1) \rangle$ and this description is unique:

$$\langle (y_1, \ldots, y_n, 1) \rangle = \langle (y_1', \ldots, y_n', 1) \rangle$$

$$\Rightarrow y_1 = y_1', \ldots, y_n = y_n'.$$

So we get a bijection b/w $k^n$ and the set of 1d subspaces of $k^{n+1}$ of the form $\langle (x_1, \ldots, x_{n+1}) \rangle$ with $x_{n+1} \neq 0$. If $x_{n+1} = 0$, then $p$ is really a 1d subspace of $k^n$, where

$$k^n \cong \{(x_1, \ldots, x_n, 0) : x_i \in k\}$$

So we get a bijection

$$KP^n \cong K^n + KP^{n-1}$$

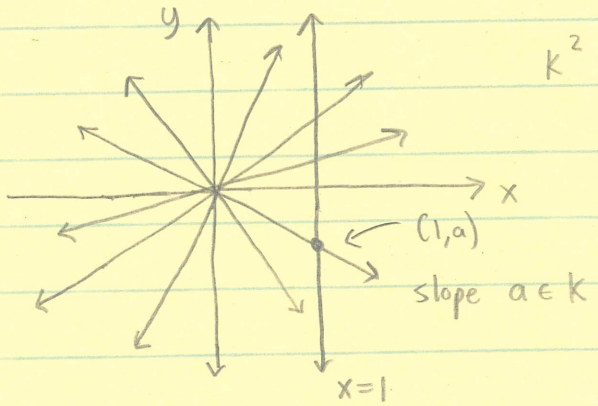
By induction, we have

$$KP^n \cong K^n + K^{n-1} + \cdots + \underbrace{K^0}_{= \{0\}}.$$

□

Examples:

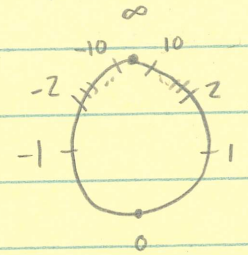
1) The projective line $KP^1$ is in 1-1 correspondence with the affine line $\mathbb{A}^1_K$ disjoint union $K^0$ (here $\mathbb{A}^1_K = K^1$)



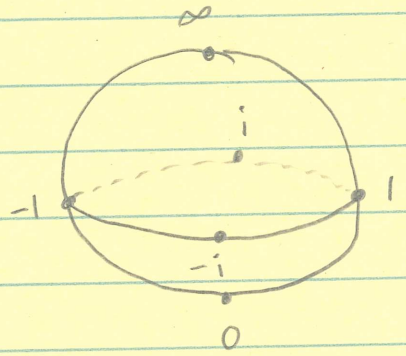

The non-vertical lines have slopes determined by elements of K. So $KP^1$ is K together with the "point at infinity" $\infty$ corresponding to the vertical line. So

$$KP^1 = K + \{\infty\}$$

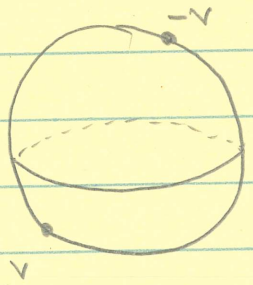
2) $\mathbb{RP}^1$ as a set is $\mathbb{R} + \{\infty\}$. But as a top'l space, it's $S^1$, the one-point compactification of $\mathbb{R}$:




3) $\mathbb{CP}^1$, the complex projective line, is $\mathbb{C} + \{\infty\}$. As a space this is $S^2$, or as a complex variety, the Riemann sphere:

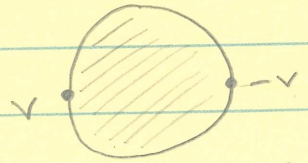



4) $\mathbb{RP}^2$, the real projective plane, is homeomorphic to $S^2/\{v \sim -v\}$



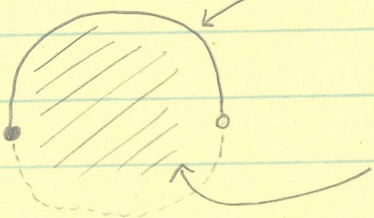

antipodal points identified

or just the northern hemisphere, a disc $D^2$:




with $v \sim -v$ for points on the boundary

This is in bijection with:




$\mathbb{RP}^1$ – "the projective line at infinity"

$$\mathbb{RP}^2 \cong \mathbb{R}^2 + \mathbb{R} + \{\infty\}$$

"the line at infinity"

"the point at infinity"

5) Any finite field $K$ has $q$ elements, where $q$ is a prime power

$$q = p^n$$

where $p$ is a prime number and $n = 1, 2, \ldots$

Moreover, all fields with $q$ elements are isomorphic, so we write $\mathbb{F}_q$ for "the" field with $q$ elements are isomorphic.

not canonically isomorphic

When $p$ is prime, $\mathbb{F}_p$ is just $\mathbb{Z}/p\mathbb{Z}$ with the usual $+, \cdot$. To get $\mathbb{F}_{p^n}$ with $n > 1$, take $\mathbb{F}_p$ and throw in all the $n$ roots of some deg. $n$ polynomial that has no roots in $\mathbb{F}_p$.

What's the cardinality of $\mathbb{F}_q P^n$?

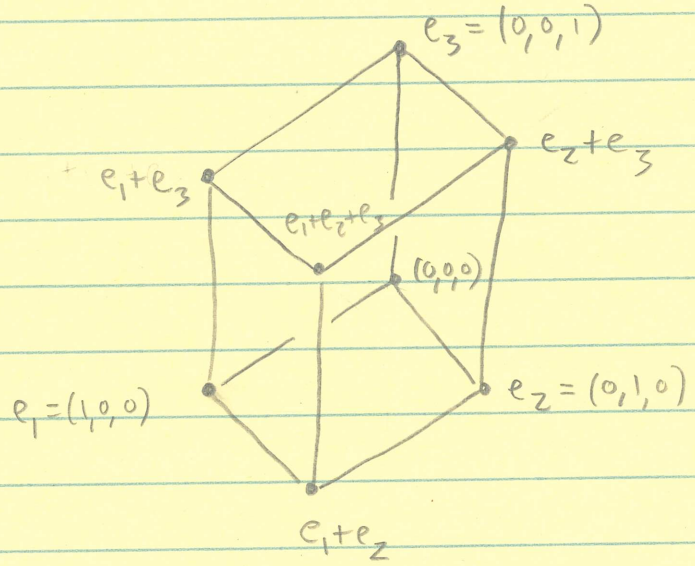
$$|\mathbb{F}_q P^n| = |\mathbb{F}_q^n + \mathbb{F}_q^{n-1} + \cdots + \mathbb{F}_q^0|$$

$$= \sum_{i=0}^{n} |\mathbb{F}_q^i| = q^n + q^{n-1} + \cdots + 1 = \frac{q^{n+1}-1}{q-1}$$

is called the q-integer $[n+1]_q$ (since it approaches $n+1$ as $q \to 0$).

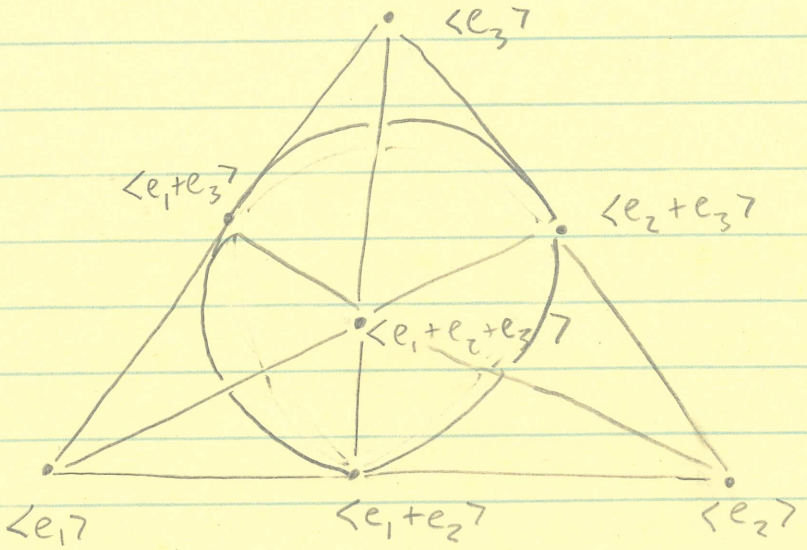
6) $\mathbb{F}_2 P^2$ is called the Fano plane - the smallest projective plane.

$|\mathbb{F}_2 P^2| = 2^2 + 2 + 1 = 7$, so it has 7 points.




$\mathbb{F}_2^3$

The Fano plane:




e.g., $\langle e_1 \rangle$, $\langle e_1+e_2 \rangle$, $\langle e_2 \rangle$ all lie on a line since they're in a 2d space $\langle e_1, e_2 \rangle$

So $\mathbb{F}_2 P^2$ has 7 points and 7 lines,

**Thm:** In any projective plane $KP^2$:

1) For any 2 distinct points $p, p'$, $\exists!$ line $\ell$ with $p, p' \leq \ell$
2) For any 2 distinct lines $\ell, \ell'$, $\exists!$ point $p$ with $p \leq \ell, \ell'$.

**Proof:** 1) Given 2 distinct 1d-subspaces of $K^3$, $p$ and $p'$, the subspace sum $p+p' = \{v+v' : v \in p, v' \in p'\}$ is 2-dim'l, so it's a line $\ell$ with $p, p' \leq \ell$ and it's the unique one.

2) Given 2 distinct 2d-subspaces of $K^3$, $\ell$ and $\ell'$, we claim $\ell \cap \ell'$ will be a 1d-subspace $p = \ell \cap \ell'$. This follows from $3 = \dim(\ell + \ell') = \dim(\ell) + \dim(\ell') - \dim(\ell \cap \ell')$

$= 2 + 2 - \dim(\ell \cap \ell')$.

Thus $\dim(\ell \cap \ell') = 1$. So $p = \ell \cap \ell'$ is a point on both lines, and we can show it's unique.

□

## Axiomatic Projective Geometry

**Def:** An *abstract projective plane* consists of a set $P$ of points, a set $L$ of *lines*, and an incidence relation $I \subseteq P \times L$. If $(p, \ell) \in I$, we say $p \, I \, \ell$ or $p$ *lies on* $\ell$. We demand:

1) For any distinct $p, p' \in P$, $\exists! \, \ell \in L$ with $p \, I \, \ell$, $p' \, I \, \ell$

2) For any distinct $\ell, \ell' \in L$, $\exists! \, p \in P$ with $p \, I \, \ell$, $p \, I \, \ell'$.

3) Nondegeneracy axiom:

$\exists$ exist 4 points, no 3 of which lie on the same line.

This is equivalent to the following statement:

3)': $\exists$ exist 4 lines, no 3 of which contain the same point.

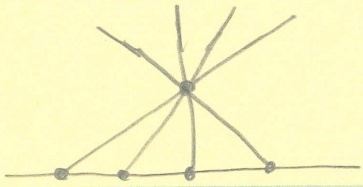
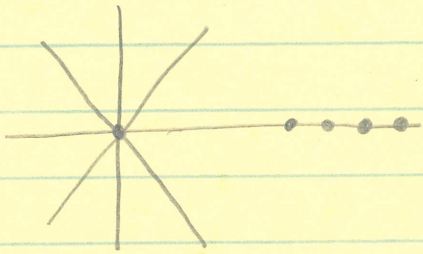
The nondegeneracy eliminates these:

1) $P = L = \phi$

2) $P = \bullet$, $L = \phi$ or $P = \phi$, $L = |$

3)

4)

5) 

6)